受領書

平成１１年　６月１８日
特　許　庁　長　官

識別番号　　１００００７８８６８
氏名（名称）　　河野　登夫　　殿
提出日　　平成１１年　６月１８日

以下の書類を受領しました。

項番	書類名	整理番号	受付番号	出願番号通知（事件の表示）
1	特許願	20348	59900586805	特願平11-173338
2	特許願	20328	59900586808	特願平11-173339

以　上

2000204540

提出日　平成１１年　６月１８日

整理番号＝２０３４８　　頁：　1/　2

【書類名】　特許願

【整理番号】　２０３４８

【提出日】　平成１１年　６月１８日

【あて先】　特許庁長官殿

【国際特許分類】　Ｇ０９Ｃ　１／００

Ｈ０４Ｋ　１／００

【発明の名称】　暗号化方法

【請求項の数】　３

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【特許出願人】

【識別番号】　０００００６２９７

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　５９７００８６３６

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　１０００７８８６８

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　０６－６９４４－４１４１

【手数料の表示】

【予納台帳番号】　００１８８９

【納付金額】　２１０００

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　９８０５２８３

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法

【特許請求の範囲】

【請求項１】　暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、公開鍵ベクトルとの積和演算結果に基づいて暗号文を得る暗号化方法において、前記積和演算結果を複数組作成し、作成した複数組の積和演算結果を多重化して、暗号文を得ることを特徴とする暗号化方法。

【請求項２】　暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、公開鍵ベクトルとを使用して、積和型の暗号文を得る暗号化方法において、前記公開鍵ベクトルに複数の乱数を多段化演算した演算結果を用いて暗号文を得ることを特徴とする暗号化方法。

【請求項３】　積和型の暗号文を得る暗号化方法において、暗号化すべき平文を誤り訂正符号化した符号語ベクトルと公開鍵ベクトルとによる積和演算により暗号文を得ることを特徴とする暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、平文を暗号文に変換するための暗号化方法に関し、特に、積和型暗号を作成する暗号化方法に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上

主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

【発明が解決しようとする課題】

公開鍵暗号系の１つである、整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、多進法を用いることにより、高速な復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特願平10－262036

号）。

【０００７】

この暗号化方法は、暗号化すべき平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，…，m_K）と基数ベクトルＢ＝（B_1，B_2，…，B_K）とを用いて暗号文Ｃ＝$m_1 B_1 + m_2 B_2 + \cdots + m_K B_K$を得る際に、$B_i$（$1 \leqq i \leqq K$）を、基数$b_i$を用いて$B_i = b_1 b_2 \cdots b_i$に、または、基数$b_i$，乱数$v_i$を用いて$B_i = v_i b_1 b_2 \cdots b_i$に設定することを特徴としている。このようにして、平文を多進法を用いて表現するようにしたので、高速な復号を行うことができる。

【０００８】

また、ＬＬＬ（Lenstra-Lenstra-Lovasz）法による攻撃に強くすることを目的として、上記暗号化方法の改良方法を提案している（特願平11－105815号、以下これを先行例という）。この暗号化方法は、暗号化すべき平文をＪ分割した平文ベクトルｍ＝（m_1，m_2，…，m_J）及び任意の乱数ベクトルｒ＝（r_{J+1}，r_{J+2}，…，r_K）と、基数b_i（$1 \leqq i \leqq K$）を用いて$B_i = b_1 b_2 \cdots b_i$に、または、基数b_i，乱数v_iを用いて$B_i = v_i b_1 b_2 \cdots b_i$に設定された基数ベクトルＢ＝（$B_1$，$B_2$，…，$B_K$）とを用いて、暗号文Ｃ＝$m_1 B_1 + m_2 B_2 + \cdots + m_J B_J + r_{J+1} B_{J+1} + r_{J+2} B_{J+2} + \cdots + r_K B_K$を得ることを特徴としている。このようにして、平文に冗長性を持たせることにより、密度（入力平文長／暗号文長）を１以上に設定でき、ＬＬＬ法などの攻撃に強くできる。

【０００９】

本発明者等は、平文に冗長性を持たせた積和型暗号の改良を研究し続けており、特に、ＬＬＬ法などの攻撃に強い改良方法を研究している。

【００１０】

本発明は斯かる事情に鑑みてなされたものであり、先行例を改良して、安全性をより高めることができる暗号化方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】

請求項１に係る暗号化方法は、暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、公開鍵ベクトルとの積和演算結果に基づいて暗号文を得る暗号化方法において、前記積和演算結果を複数組作成し、作成した複数組の積和演算結果を多重化して、暗号文を得ることを特徴とする。

【００１２】

請求項２に係る暗号化方法は、暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、公開鍵ベクトルとを使用して、積和型の暗号文を得る暗号化方法において、前記公開鍵ベクトルに複数の乱数を多段化演算した演算結果を用いて暗号文を得ることを特徴とする。

【００１３】

請求項３に係る暗号化方法は、積和型の暗号文を得る暗号化方法において、暗号化すべき平文を誤り訂正符号化した符号語ベクトルと公開鍵ベクトルとによる積和演算により暗号文を得ることを特徴とする。

【００１４】

本発明では、平文に冗長性を持たせる、即ち、本来暗号化すべき平文を分割した平文ベクトル及び特に暗号化を必要としない任意のベクトルと、基数ベクトルとの積和演算によって暗号文を構成する。よって、密度を１以上に設定でき、１つの暗号文に対して非常に多くの復号方法が存在するので、ＬＬＬ法などによる攻撃は非常に困難となる。この結果、安全性は高く、しかも、多重化、多段暗号化、または、誤り訂正符号化を適用することにより、先行例より安全性が更に向上する。

【００１５】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、積和型暗号を採用した本発明及び先行例における暗号化方法をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティａ側で、暗号化器１にてメッセージｍを暗号文Ｃに暗号化し、通信路３を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂ側で、復号器２にてその暗号文Ｃを元のメッセージｍに復号する場合を示し

ている。

【００１６】

まず、平文に冗長性を持たせた積和型暗号の手法について説明する。一般に暗号文Ｃに対し、秘密の乱数ｗのＰに関する逆元w^{-1}を用いて、下記（１）のようにして中間復号文Ｍを導く。

$$w^{-1}C \equiv M \pmod{P} \qquad \cdots (1)$$

【００１７】

中間復号文Ｍは、メッセージを$\{m_i\}$、基数を$\{b_i\}$、乱数を$\{v_i\}$として、下記（２）のように表される。

$$M = m_1 v_1 b_1 + m_2 v_2 b_1 b_2 + \cdots + m_K v_K b_0 b_1 \cdots b_K \qquad \cdots (2)$$

【００１８】

ここで、基数に関して、次のように定義する。

（定義１）

$m_i < b_i$を満たす基数を正規基数、$m_i \geqq b_i$を満たす基数を退化基数とする。

（定義２）

一般に、ｉ個の基数の積$b_1 b_2 \cdots b_i$を長さｉの基数積とする。

（定義３）

基数積においてポストフィックス（postfix)に退化基数を有する基数積を退化基数積とする。退化基数積以外で基数積に退化基数を含むものを準正規基数積とする。退化基数積，準正規基数積以外の基数積を正規基数積とする。

【００１９】

また、メッセージの大きさm_iは下記（３）を満たし、正規基数b_iは下記（４）を満たす素数とする。

$$m_i < 2^{\alpha} \qquad \cdots (3)$$

【００２０】

【数１】

$$b_i = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \cdots (4)$$

【００２１】

以下、先行例に示された暗号化・復号方法を、本発明の基本方式として説明する。

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：｛b_i｝，｛v_i｝，Ｐ，ｗ（$1 \leqq i \leqq K$）

・公開鍵：｛c_i｝

【００２２】

基数積$b_1\ b_2 \cdots b_i$に乱数v_iを乗じて、基数ベクトルＢ＝（B_1，B_2，…，B_K）を下記（５）のように設定する。

$$B_i = v_i\ b_1\ b_2 \cdots b_i \qquad \cdots (5)$$

【００２３】

ここで、上記（５）で示される各成分B_iがほぼ同じ大きさになるように乱数v_iを設定する。但し、ｇｃｄ（v_i，b_{i+1}）＝１を満たすものとする。なお、ＬＬＬ法に対して高い耐性を得るために、ランダムな位置に準正規基数積または退化基数積を用いる。例えば、ｉ＝１からｉ＝Ｊまでを正規基数とし、ｉ＝Ｊ＋１から最後のｉ＝Ｋまでを退化基数とした場合には、最初のｉ＝１からｉ＝Ｊまでのメッセージは正しく復号することができる。

【００２４】

乱数ｗを用いて、公開鍵｛c_i｝を下記（６）のように求める。

$$c_i \equiv w B_i \pmod{P} \qquad \cdots (6)$$

【００２５】

暗号文Ｃは、メッセージ｛m_i｝の成分と公開鍵｛c_i｝の成分とを用いた積和演算によって与えられる。暗号文Ｃは、具体的には下記（７）のように表される。

$$C = m_1\ c_1 + m_2\ c_2 + \cdots + m_K\ c_K \qquad \cdots (7)$$

【００２６】

以下のようにして復号処理が行われる。暗号文Ｃに対して、中間復号文Ｍを下記（８）のようにして求める。

$$M \equiv w^{-1} C \pmod{P} \quad \cdots (8)$$

この中間復号文Ｍは、具体的には下記（９）として与えられるので、以下に示す逐次復号アルゴリズムによって復号できる。

$$M = m_1 v_1 b_1 + m_2 v_2 b_1 b_2 + \cdots + m_K v_K b_1 b_2 \cdots b_k \quad \cdots (9)$$

【００２７】

〔逐次復号アルゴリズム〕

ステップ１

$$M_1 = M / b_1$$

$$m_1 \equiv M_1 v_1^{-1} \pmod{b_2}$$

ステップｉ（ｉ＝２～Ｋ－１）

$$M_i = (M_{i-1} - m_{i-1} v_{i-1}) / b_i$$

$$m_i \equiv M_i v_i^{-1} \pmod{b_{i+1}}$$

ステップＫ

$$M_K = (M_{K-1} - m_{K-1} v_{K-1}) / b_K$$

$$m_K = M_K / v_K$$

【００２８】

このアルゴリズムにあっては、正規基数である場合（$m_i < b_i$）にはm_iを一意に正しく復号でき、退化基数である場合（$m_i \geqq b_i$）にはm_iを一意に正しく復号できない。よって、例えば、メッセージ｛m_i｝の最初のｉ＝１からｉ＝Ｊまでは暗号化すべき平文ベクトルを割り当て、残りのｉ＝（Ｊ＋１）からｉ＝Ｋまでは復号できなくても問題がない乱数ベクトルを割り当てれば良い。

【００２９】

次に、上述した先行例を改良した本発明の手法について説明する。

（第１実施の形態）

先行例である基本方式を複数組用意し、それらを多重化することによって暗号

文を作成する第１実施の形態について、２組の基本方式を用いる場合を例にして説明する。

【００３０】

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{b_{Pi}\}$，$\{b_{Qi}\}$，$\{v_{Pi}\}$，$\{v_{Qi}\}$，P，Q，N，w

・公開鍵：$\{c_i\}$

２つの大きな素数P，Qを選択し、それらの積をNとする。基本方式におけるK個の基数b_iの集合を２通り準備し、$\{b_{Pi}\}$，$\{b_{Qi}\}$とする。また、それらより生成した基数積に乱数$\{v_{Pi}\}$，$\{v_{Qi}\}$を乗じたものを$\{B_{Pi}\}$，$\{B_{Qi}\}$とする。中国人の剰余定理を用いて、P，Qによる余りがそれぞれB_{Pi}，B_{Qi}となるような最小の整数B_iを導く。

【００３１】

Nを法として、秘密の乱数wを用いて、基本方式と同様に、公開鍵$\{c_i\}$を下記（10）のように求める。

$$c_i \equiv w B_i \pmod{N} \qquad \cdots (10)$$

暗号化は、先行例と同様に上記（７）のように、積和演算によって実行される。但し、各メッセージの大きさは、$|m_i| = 2^e$ビットとする。

【００３２】

復号処理は、以下のようにして行われる。

暗号文Cに対して、法P，法Qにおいて、それぞれ中間復号文M_P，M_Qを下記（11），（12）のようにして求める。

$$M_P \equiv w^{-1} C \pmod{P} \qquad \cdots (11)$$

$$M_Q \equiv w^{-1} C \pmod{Q} \qquad \cdots (12)$$

【００３３】

各中間復号文M_P，M_Qに関して、下記（13），（14）が成立する。

$$M_P = m_1 B_{P1} + m_2 B_{P2} + \cdots + m_K B_{PK} \qquad \cdots (13)$$

$$M_Q = m_1 B_{Q1} + m_2 B_{Q2} + \cdots + m_K B_{QK} \qquad \cdots (14)$$

【００３４】

M_P，M_Qに対して、以下に示す逐次復号アルゴリズムを適用することによっ

て、余りのペア（$m_i^{(P)}$，$m_i^{(Q)}$）を導くことができる。但し、m_iは、下記（15），（16）の何れかであるとする。

$$m_i \equiv m_i^{(P)} \pmod{b_{Pi+1}} \quad \cdots (15)$$

$$m_i \equiv m_i^{(Q)} \pmod{b_{Qi+1}} \quad \cdots (16)$$

これらに対して中国人の剰余定理を適用すると、メッセージ$m_i < lcm(b_{Pi+1}, b_{Qi+1})$を復号することができる。

【００３５】

なお、合成数Ｎを法とするこの第１実施の形態のような多重化方式では、Ｎの素因数分解が困難である場合、Ｎを公開しても安全と考えられる。よって、そのような場合には、Ｎを法として求めた暗号文を送付するようにしても良い。

【００３６】

第１実施の形態では、平文に冗長性を持たせた状態で基数積を多重暗号化したので、レート（メッセージ総長／暗号文長）は低いが、密度（入力平文長／暗号文長）を高くした積和型暗号を実現できる。そして、基数積を多重化することにより、先行例と比べて更に高い安全性を確保している。

【００３７】

（第２実施の形態）

基数積を多段化して暗号化するようにした第２実施の形態について説明する。

基数積$b_1\ b_2 \cdots b_i$に対し、乱数ｗと素数Ｐとの組（ｗ，Ｐ）をＳ組選択し、下記（17-1），（17-2），・・・，（17-S）のようにＳ段にわたって乱数を乗じていくことにより、最終的に得られる$B_i^{(S)}$を公開鍵c_iとする。

$$b_1\ b_2 \cdots b_i\ w^{(1)} \equiv B_i^{(1)} \pmod{P_1} \quad \cdots (17\text{-}1)$$

$$B_i^{(1)}\ w^{(2)} \equiv B_i^{(2)} \pmod{P_2} \quad \cdots (17\text{-}2)$$

$$\vdots \qquad\qquad \vdots$$

$$B_i^{(S-1)}\ w^{(S)} \equiv B_i^{(S)} \pmod{P_S} \quad \cdots (17\text{-}S)$$

【００３８】

但し、Ｓ個の素数P_1，P_2，…，P_Sについては、下記（18）の条件を満たすものとする。下記（18）は、復号を補償した上でP_iがP_{i+1}より小さいこと

を意味する。また、これらの素数P_1，P_2，…，P_sは全て秘密にする。

【００３９】

【数２】

$$P_1 \lesssim P_2 \lesssim \cdots \lesssim P_s \quad \cdots (18)$$

【００４０】

なお、素数P_1，P_2，…，P_sをすべて秘密にしたが、素数P_sのみを公開して、P_sを法とした暗号文を用いる手法も可能である。

【００４１】

第２実施の形態でも、平文に冗長性を持たせた状態で多段暗号化したので、低レートではあるが、高い密度の積和型暗号を実現できる。そして、暗号文を作成する際の多段化の複雑さによって、先行例より高い安全性を確保している。

【００４２】

（第３実施の形態）

誤り訂正符号化を利用した第３実施の形態について説明する。

図２は、この第３実施の形態をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図であり、図１と同一部分には同一番号，同一記号を付している。送信側のエンティティａには、メッセージｍを誤り訂正符号化する誤り訂正符号符号化器11と、得られた符号語ｃを用いて積和型の暗号文Ｃを作成する積和型暗号暗号化器12とが設けられ、受信側のエンティティｂには、暗号文Ｃを元の符号語ｃに復号する積和型暗号復号器21と、符号語ｃを元のメッセージｍに復号する誤り訂正符号復号器22とが設けられている。なお、誤り訂正符号としては、最大距離分離符号であるReed-Solomon符号を使用する。

【００４３】

メッセージｍの長さをL_mビット、これに対応する誤り訂正符号の符号長をL_{EC}ビット、この符号長L_{EC}ビットを有する符号語ｃに対応する暗号文ＣのサイズをL_Cビットとした場合に、下記（19）の関係が成り立つ。

$$L_m < L_C < L_{EC} \quad \cdots (19)$$

【００４４】

第３実施の形態では、基数の添字の集合｛ｉ｝の中からランダムにnt個を選択し、選択したこのnt個の添字ｉに対応する基数b_iを退化基数に設定し、残りの基数は正規基数とする。

【００４５】

誤り訂正符号理論により、以下の定理が成立する。

（定理１）

退化基数積に対応するメッセージは歪み、その結果、符号語ｃに長さｅ以下の単一消失バースト誤りが生起する。

（定理２）

ｔ重の消失バースト誤りの総長がＧＦ（2^s）上のシンボル単位でＢである場合、ＧＦ（2^s）上のReed-Solomon符号に要求される検査記号数はＢに等しい。

【００４６】

次に、第３実施の形態における具体例を説明する。

メッセージ長を$|m_i| = 2^{64}$、正規基数b_i，退化基数b_i'をそれぞれ下記（20），（21）とする。但し、下記（22）の条件を満たすとする。

$$b_i = 2^{64} + \delta_i \quad (1 \leqq i \leqq 25) \quad \cdots (20)$$

$$b_i' = 2^{32} + \delta_i' \quad (26 \leqq i \leqq 32) \quad \cdots (21)$$

【００４７】

【数３】

$$1 \ll \delta_i \ll 2^{64}, 1 \ll \delta_i' \ll 2^{32} \quad \cdots (22)$$

【００４８】

ＧＦ（2^s）上のReed-Solomon符号を用いる場合、メッセージ長L_m，誤り訂正符号符号長をL_{EC}，暗号文長L_Cを求めると、それぞれ下記（23），（24），（25）のようになる。そして、それらの値からレートｒ，密度ρを算出すると、

それぞれ下記（26），（27）となる。

$$L_m = 26 \times 64 = 1664 \text{（ビット）} \quad \cdots (23)$$

$$L_{EC} = 256 \times 8 = 2048 \text{（ビット）} \quad \cdots (24)$$

$$L_c = 64 \times 29 + \log_2 32 = 1861 \text{（ビット）} \quad \cdots (25)$$

$$r = 1664 / 1861 = 0.894 \quad \cdots (26)$$

$$\rho = 2048 / 1861 = 1.10 \quad \cdots (27)$$

【００４９】

第３実施の形態では、誤り訂正符号を利用したので、レートは低くなるが、高い密度の積和型暗号を構成できる。また、誤り訂正符号化によって、送信側のエンティティ自身にあっても、退化基数積の位置が不明になるので、極めて高い安全性を確保できる。

【００５０】

図３は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、第３実施の形態において、メッセージｍを符号語ｃに誤り訂正符号化する処理、及び、符号語ｃを用いて積和型の暗号文Ｃを作成する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ40は、送信側のエンティティに設けられている。

【００５１】

図３において、コンピュータ40とオンライン接続する記録媒体41は、コンピュータ40の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体41には前述の如きプログラム41a が記録されている。記録媒体41から読み出されたプログラム41a がコンピュータ40を制御することにより、コンピュータ40が誤り訂正符号化を用いて暗号文Ｃを作成する。

【００５２】

コンピュータ40の内部に設けられた記録媒体42は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体42には前述の如きプログラム42a が記録されている。記録媒体42から読み出されたプログラム42a がコンピュータ40を制御することにより、コンピュータ40が誤り訂正符号化を用

いて暗号文Ｃを作成する。

【００５３】

コンピュータ40に設けられたディスクドライブ40a に装填して使用される記録媒体43は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体43には前述の如きプログラム43a が記録されている。記録媒体43から読み出されたプログラム43a がコンピュータ40を制御することにより、コンピュータ40が誤り訂正符号化を用いて暗号文Ｃを作成する。

【００５４】

なお、上述した例では、暗号通信システムの場合について説明したが、平文を暗号化して暗号文を作成し、作成した暗号文を単に記録するような場合にも、本発明の暗号化方法を適用できることは勿論である。

【００５５】

【発明の効果】

以上のように、本発明では、平文に冗長性を持たせるようにした先行例を改良したので、大きな密度を維持して、ＬＬＬ法などの攻撃に対する安全性を先行例より更に向上することが可能となる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【００５６】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、基数 b_i （$1 \leqq i \leqq K$）を用いて第ｉ成分 $B_i = b_1\ b_2 \cdots b_i$ に設定された基数ベクトルとの積和演算結果に基づいて暗号文を得る暗号化方法において、前記積和演算結果を複数組作成し、作成した複数組の積和演算結果を多重化して、暗号文を得る暗号化方法。

（２）　暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、基数 b_i （$1 \leqq i \leqq K$）を用いて第ｉ成分 $B_i = b_1\ b_2 \cdots b_i$ に設定された基数ベクトルとを使用して、積和型の暗号文を得る暗号化方法において、前記 B_i に複

数の乱数を多段化演算した演算結果を用いて暗号文を得る暗号化方法。

（３）　基数b_i（$1 \leqq i \leqq K$）を用いて第ｉ成分$B_i = b_1\ b_2 \cdots b_i$に設定された基数ベクトルを使用して、積和型の暗号文を得る暗号化方法において、暗号化すべき平文を誤り訂正符号化した符号語ベクトルと前記基数ベクトルとによる積和演算により暗号文を得る暗号化方法。

（４）　暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、基数b_i，乱数v_i（$1 \leqq i \leqq K$）を用いて第ｉ成分$B_i = v_i\ b_1\ b_2 \cdots b_i$に設定された基数ベクトルとの積和演算結果に基づいて暗号文を得る暗号化方法において、前記積和演算結果を複数組作成し、作成した複数組の積和演算結果を多重化して、暗号文を得る暗号化方法。

（５）　暗号化すべき平文を分割した平文ベクトル及び任意のベクトルと、基数b_i，乱数v_i（$1 \leqq i \leqq K$）を用いて第ｉ成分$B_i = v_i\ b_1\ b_2 \cdots b_i$に設定された基数ベクトルとを使用して、積和型の暗号文を得る暗号化方法において、前記B_iに複数の乱数を多段化演算した演算結果を用いて暗号文を得る暗号化方法。

（６）　基数b_i，乱数v_i（$1 \leqq i \leqq K$）を用いて第ｉ成分$B_i = v_i\ b_1\ b_2 \cdots b_i$に設定された基数ベクトルを使用して、積和型の暗号文を得る暗号化方法において、暗号化すべき平文を誤り訂正符号化した符号語ベクトルと前記基数ベクトルとによる積和演算により暗号文を得る暗号化方法。

（７）　複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１～３，（１）～（６）の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備える暗号通信システム。

（８）　請求項１～３，（１）～（６）の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を記録する記録器とを備える暗号化・記録装置。

（９）　平文から積和型の暗号文を得る暗号化装置において、暗号化すべき平文を誤り訂正符号化して符号語ベクトルを得る誤り訂正符号符号化器と、該符号化

器にて得られる符号語ベクトルと、基数b_i（$1 \leqq i \leqq K$）を用いて第i成分$B_i = b_1\ b_2 \cdots b_i$に設定された基数ベクトルとの積和演算によって暗号文を得る積和型暗号暗号化器とを備える暗号化装置。

(10)　コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を誤り訂正符号化して符号語ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、符号語ベクトルと基数b_i（$1 \leqq i \leqq K$）を用いて第i成分$B_i = b_1\ b_2 \cdots b_i$に設定された基数ベクトルとの積和演算によって暗号文を得ることをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図２】

２人のエンティティ間における情報の他の通信状態を示す模式図である。

【図３】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

1　暗号化器

2　復号器

3　通信路

11　誤り訂正符号符号化器

12　積和型暗号暗号化器

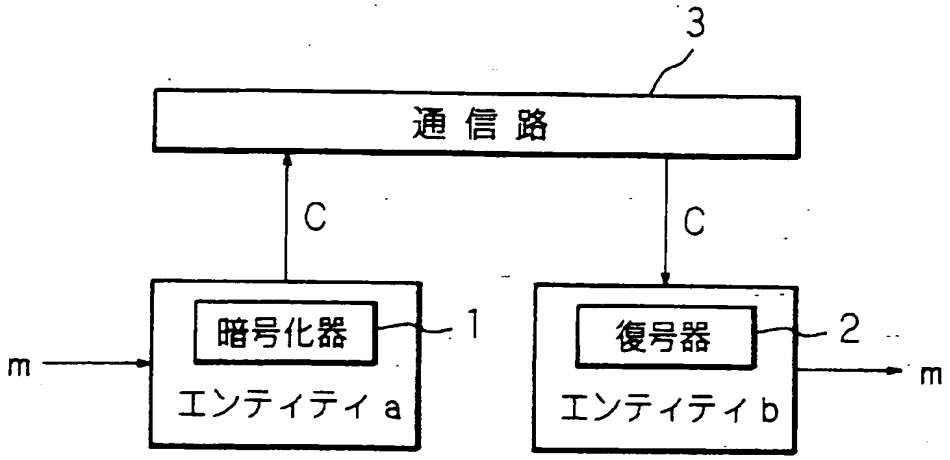
40　コンピュータ

41，42，43　記録媒体

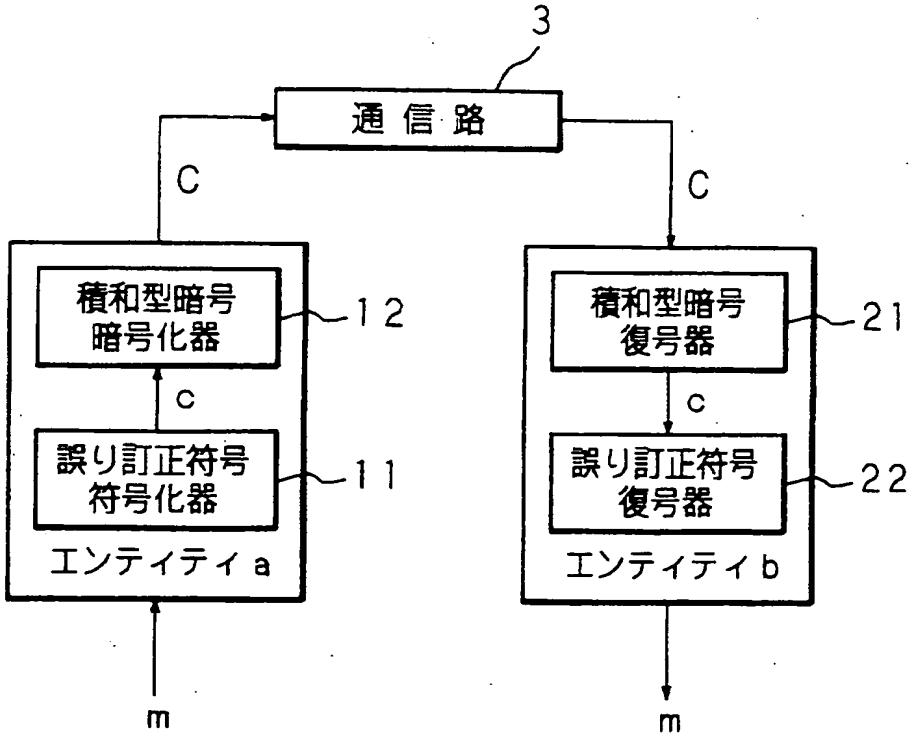
a，b　エンティティ

【書類名】　　図面

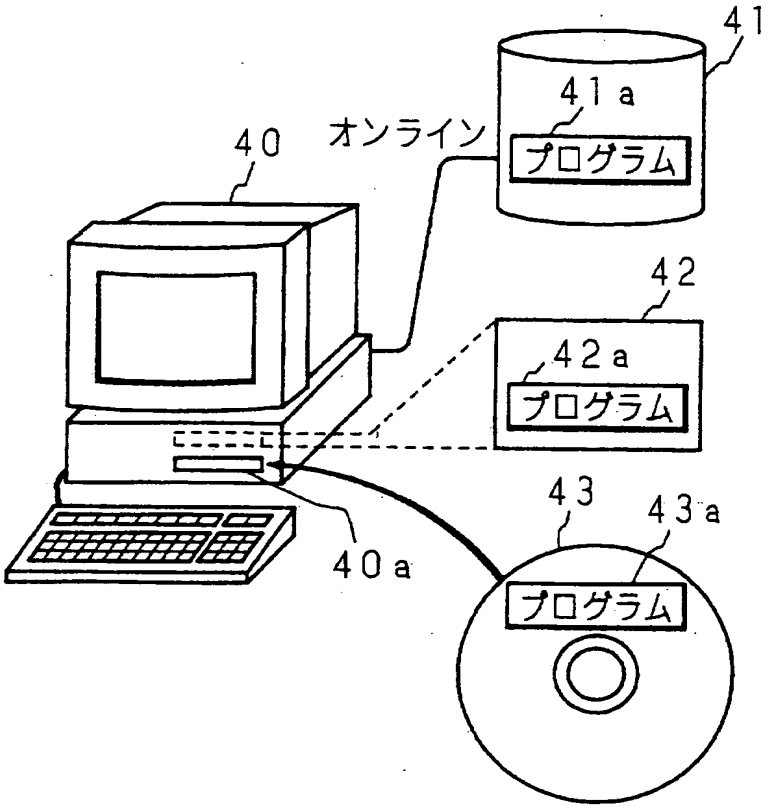
【図１】


3
通信路
C
C
暗号化器
1
復号器
2
m
m
エンティティａ
エンティティｂ

【図２】


3
通信路
C
C
積和型暗号
暗号化器
12
c
誤り訂正符号
符号化器
11
積和型暗号
復号器
21
c
誤り訂正符号
復号器
22
エンティティａ
エンティティｂ
m
m

【図３】



【書類名】　　要約書

【要約】

【課題】　密度（入力平文長／暗号文長）が高く、ＬＬＬ法などの攻撃に対する安全性が高い積和型暗号の暗号化方法を提供する。

【解決手段】　暗号化すべき平文を含むメッセージを誤り訂正符号化して得られる符号語ベクトルと、基数b_i（$1 \leqq i \leqq K$）を用いて第ｉ成分$B_i = b_0 \cdot b_1 \cdots b_i$に設定された基数ベクトルとを利用して、積和型暗号の暗号文を作成する。

【選択図】　　図１